경량화된 환자-헬스케어 인증 프로토콜에 대한 추적가능성 분석

류현호*, (교신저자)김현성*,**
*경일대학교 컴퓨터사이언스학부,
** 말라위대학교 수학과

ryoofamily0430@gmail.com, kim@kiu.ac.kr

Traceability Cryptanalysis on Lightweight Patient-Healthcare Authentication Protocol

Hyunho Ryu*, (Corresponding Author)Hyunsung Kim*,**
*School of Computer Science, Kyungil University,
**Mathematical Science Department, CHANCO, University of Malawi

요 약

소형화되는 센서 기술 및 무선 통신 기술의 발달로 인한 사물인터넷을 기반 원격헬스케어를 위한 다양한 연구들이 진행되고 있다. 특히, 원격헬스케어 서비스는 환자의 민감 정보인 건강기록을 다루기 때문에 보안 및 프라이버시에 대한 요구사항이 다른 응용보다 더 중요하게 고려되고 있다. 이를 위해 최근에 Alzahrani 등은 원격헬스케어를 위한 경량화된 환자-헬스케어 인증 프로토콜을 제안하였다. 하지만, 본 논문에서는 Alzahrani 등의 프로토콜이 비추적성을 제시하지 못하는 문제를 Canetti-Krawczyk 모델에 기반한 BAN 로직 분석을 통해 증명한다. 또한, 이들 프로토콜에 존재하는 문제를 해결하기 위한 해결 방안에 대해 간략한 개요를 제시한다.

Ⅰ. 서 론

무선인체통신망(Wireless Body Area Network)은 인체 주변 통신 환경에서 다양한 센서 장치들을 연결하는 근거리 무선 통신 기술이다[1]. 무선인체통신망 기술을 활용한 헬스케어 시스템을 위한 다양한 보안과 프라이버시를 위한 연구가 진행되었다[2-4]. 특히, 원격헬스케어 서비스에 있어서 환자의 개인정보에 대한 보안 및 프라이버시는 아주 중요한 요구사항이다. 최근에 Alzahrani 등은 무선인체통신망 상에서 경량화된 환자-헬스케어 인증 프로토콜을 제안하였다[3]. 보안 증명을 위해 BAN 로직과 자동화된 시뮬레이션 툴상에서의 정형화된 분석을 제시하였다[4]. 하지만, 본 논문에서는 Alzahrani 등의 인증 프로토콜이 비추적성을 제시하지 못하는 문제를 Canetti-Krawczyk(CK) 모델 기반 BAN 로직 분석을 통해 증명한다[5]. 특히, BAN 로직을 통해 네트워크 참여자의 식별자 추적 문제로 인해 메시지의 신선성(Freshness)을 제시하지 못하는 문제를 도출한다.

Ⅱ. Alzahrani 등의 환자-헬스케어 인증 프로토콜

Alzahrani 등의 인증 프로토콜은 초기화, 등록, 인증 및 전송 단계로 구성된다[3]. 각 단계는 다음과 같다.

초기화 단계: 서버관리자(Server Administrator, SA)는 마스터키인 KS_{HN}을 생성하고, HN 의 메모리에 저장한다.

등록 단계: 1) SA 는 id_S 를 선택하고 센서 노드 SN 을 위한 난수 a, S_{P1}, S_{P2} 를 생성 후 $<id_S, S_{P1}, S_{P2}>$를 HN 의 메모리에 저장한다. 2) SA 는 $x_{SN}=a \oplus KS_{HN}$ 과 $y_{SN}=ids \oplus h(KS_{HN}, a)$를 계산하고 $<id_S, x_{SN}, y_{SN}, S_{P1}, S_{P2}>$를 SN 의 메모리에 저장한다. 3) SA 는 환자의 액세스포인트 AP 의 아이디인 id_A 를 선택하여 HN 의 메모리에 저장한다.

인증 단계: 그림 1 과 같이 환자의 SN 은 HN 에게 인증을 요청한다. 인증이 성공하면 HN 은 세션키 K_s 를 SN 과 같이 생성해서 뒤따르는 데이터의 안전성을 위해 사용한다.

Ⅲ. 추적가능성에 대한 BAN 로직 분석

Alzahrani 등의 프로토콜에 대한 취약성 분석을 위해 CK 보안 모델에 기반한 BAN 로직 분석을 제시한다[4-5]. 특히 분석의 목적은 Alzahrani 등의 인증 프로토콜이 환자의 AP 가 세션마다 동일한 식별자인 id_A 를 사용하는 문제를 통해 도출할 수 있다. 즉, AP 의 메시지에 대한 신선성을 제시하지 못하는 문제를 도출한다.

CK 위협 모델: 프로토콜에 대한 분석을 위해서 다양한 보안 프로토콜의 분석에 널리 사용되는 CK 위협 모델을 적용한다[5]. CK 모델에서 공격자는 전송되는 메시지의 도청, 변경, 결정, 삽입에 의한 통신 채널을 제어할 수 있다. 또한, 명시적 공격(Explicit attack)을 통해 네트워크 참여자의 메모리에 저장된 비밀 정보를 획득할 수 있다. 그러므로 인증 프로토콜의 보안은 세션비밀들과 같은 개인 값들의 노출이 다른 세션의 보안과 통신 참여자들의 다른 개인 정보에 영향을 최소한으로 제시되도록 설계되어야 한다.

BAN 로직 분석: BAN 로직의 기본 규칙 및 기호는 페이지 제약으로 인해 논문[4]의 내용으로 대체한다. 일반적인 BAN 로직의 목적은 상호인증과 안전한 세션키 동의에

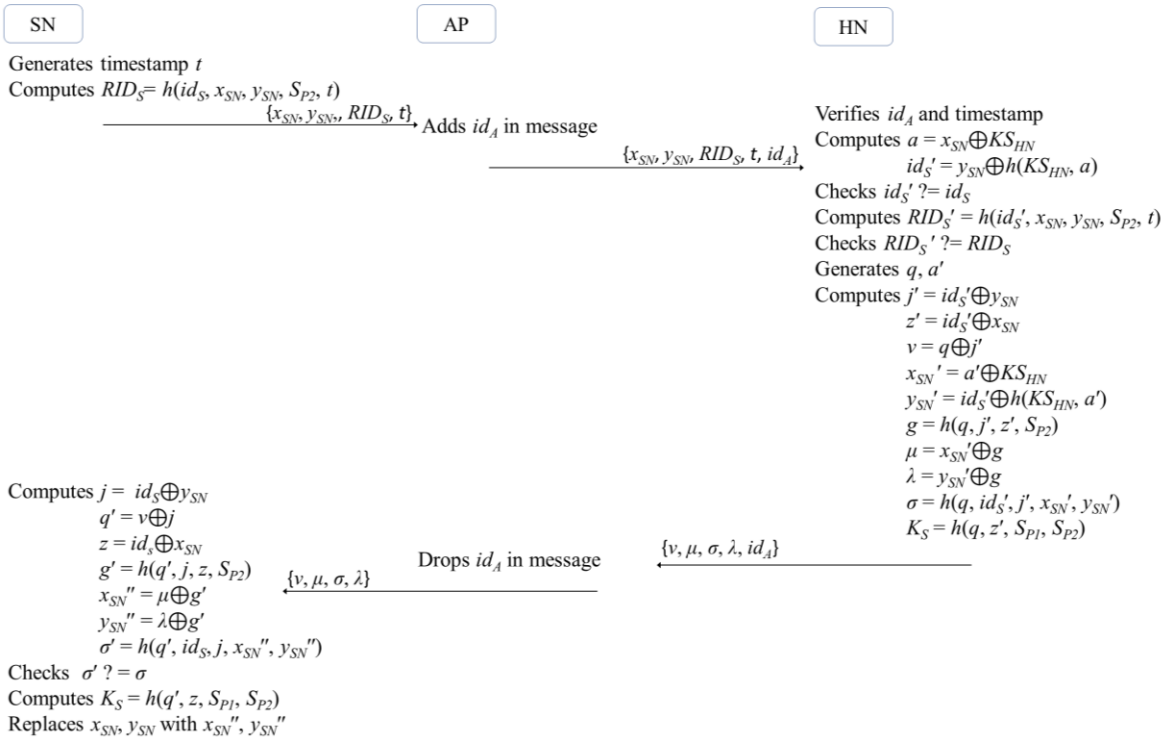

그림 1. Alzahrani 등의 인증 프로토콜의 인증 단계

있다. 본 논문에서는 Alzahrani 등의 프로토콜에 대한 추적가능성 검증에 있으므로 AP 의 식별자인 id_A 에 대한 신선성에 초점을 맞춘다.

Goal 1: HN| ≡#(id_A)

Idealized form: 그림 1 로부터 SN, AP, HN 사이의 전송되는 메시지를 다음과 같이 변형한다.

M1. SN→AP: $<X_{SN}>_{KS_{HN}}$, $<Y_{SN}>_{KS_{HN}}$, $<RIDs>_{KS_{HN}}$, T

M2. AP→HN: $<X_{SN}>_{KS_{HN}}$, $<Y_{SN}>_{KS_{HN}}$, $<RIDs>_{KS_{HN}}$, T, id_A

Assumptions: 증명을 위한 가정은 다음과 같다.

A1: HN| ≡HN$\overset{X_{SN}}{\longleftrightarrow}$SN

Proof: 최종목표를 달성하는지 증명하기 위해 그림 1 에서 주고받은 메시지를 통해 규칙과 가정을 이용하여 목표 달성 여부를 판별한다.

M1 을 통해 다음 단계를 구성할 수 있다:

단계 1. AP⊲($<X_{SN}>_{KS_{HN}}$, $<Y_{SN}>_{KS_{HN}}$, $<RIDs>_{KS_{HN}}$, T)

단계 1 을 기반으로 AP 는 메시지에 id_A 를 추가하여 HN 에게 전송한다.

M 2 를 기반으로 다음 단계를 구성할 수 있다:

단계 2. HN⊲($<X_{SN}>_{KS_{HN}}$, $<Y_{SN}>_{KS_{HN}}$, $<RIDs>_{KS_{HN}}$, T, id_A)

A1 과 메시지 의미 규칙을 통해 다음을 유도한다:

단계 3. HN| ≡AP| ~($<X_{SN}>_{KS_{HN}}$, $<Y_{SN}>_{KS_{HN}}$, $<RIDs>_{KS_{HN}}$, T, id_A)

A2, A3, 신선성 규칙으로부터 다음을 유도할 수 있어야 한다.

단계 4. HN| ≡#($<X_{SN}>_{KS_{HN}}$, $<Y_{SN}>_{KS_{HN}}$, $<RIDs>_{KS_{HN}}$, T, id_A)

하지만 단계 4 를 만족하기 위해서는 HN 이 메시지 내부에 존재하는 모든 요소에 대한 신선성을 통해 세션마다 다른 값을 확인할 수 있어야 한다. 하지만 AP 가 세션마다 동일한 id_A 를 이용하므로 이를 달성하지 못한다. 즉, CK 모델에 기반한 공격자는 id_A 를 통해 이전 세션의 동일한 id_A 를 가진 메시지를 통해서 환자가 누군지 모르지만 동일한 환자로부터 전송된 메시지인지 여부를 확인할 수 있다. 즉, CK 모델의 공격자는 id_A 를 통해 통신 세션을 추적할 수 있고, 그렇게 함으로서 환자의 프라이버시를 보증할 수 없다.

Ⅳ. 결론 및 고찰

본 논문에서는 Alzahrani 등의 인증 프로토콜에 대한 추적가능성 문제를 CK 모델에 기반한 BAN 로직 분석을 통해 보였다. 즉, Alzahrani 등의 인증 프로토콜은 프라이버시에 대한 요구사항 중 비추적성을 제공하지 못하는 문제가 있다. 이에 대한 해결책은 모든 네트워크 참여자들이 동적식별자를 사용하여 세션별 사용하는 식별자에 신선성을 제공할 수 있는 프로토콜 설계로 해결할 수 있을 것이다. 해결방안은 향후 연구로 제시하고자 한다.

ACKNOWLEDGMENT

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

참 고 문 헌

[1] Y. M. Park, "A Study on the Implementation of WBAN-Based Medical Gateway," Journal of Advanced Navigation Technology, vol. 18, no. 6, pp. 640-647, 2014.

[2] B. Pradhan, S. Bhattacharyya, K. Pal, "IoT-based Applications in Healthcare Devices," Journal of Healthcare Engineering, vol. 2021, Article ID 6632599, 2021.

[3] B. A. Alzahrani, A. Irshad, A. Albeshri, K. Alsubhi, "A Provably Secure and Lightweight Patient-Healthcare Authentication Protocol in Wireless Body Area Networks," Wireless Personal Communications, vol. 117, pp. 47-69, 2021.

[4] B. Kapito, M. Nyirenda, H. Kim, "Privacy Preserving Machine Authenticated Key Agreement for Internet of Things," International Journal of Computer Networks & Communications, vol. 13, no. 2, pp. 99-120, 2021.

[5] R. Canetti, H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," Advances in Cryptology, pp. 453-474, 2001.